

Your Ref: 0023-0209JP

Our Ref: PA1120

**Translation of Selected Portions of  
Pat. Laid-open Official Gazette**

-----  
Appln. No: 11-15683  
Appln. Date: January 25, 1999  
Laid-open Pub. No: 11-316677  
Laid-open Pub. Date: November 16, 1999  
Priority: 1/29/98 U.S.S.N. 09/015563

Inventor(s): Eric Grosse  
Applicant(s): Lucent Technologies Inc.  
Attorney(s): Hirofumi Mitsumata  
-----

1. Title of the Invention

SECURITY METHOD OF A COMPUTER NETWORK





2. Claims

(omitted)

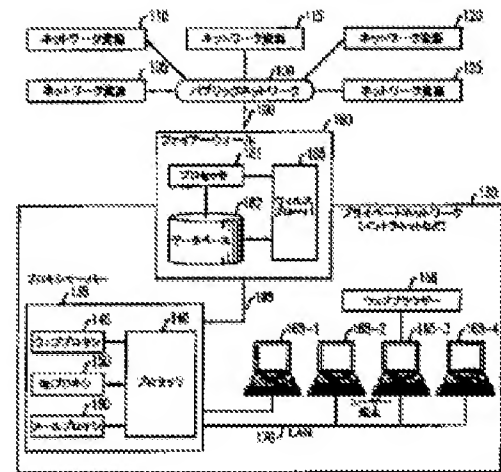
3. Detailed Description of the Invention (Selected Portions)

1)

(omitted)

**METHOD FOR SECURING COMPUTER NETWORK****Publication number:** JP11316677**Publication date:** 1999-11-16**Inventor:** GROSSE ERIC**Applicant:** LUCENT TECHNOLOGIES INC**Classification:****- international:** G06F21/22; G06F13/00; G06F21/00; H04L29/06; G06F21/22; G06F13/00; G06F21/00; H04L29/06; (IPC1-7): G06F9/06; G06F13/00; G06F15/00; H04L12/26**- European:** H04L29/06S14D1; H04L29/06**Application number:** JP19990015683 19990125**Priority number(s):** US19980015563 19980129**Also published as:** EP0936787 (A2)  
 US6205551 (B1)  
 EP0936787 (A3)  
 CA2254707 (A1)  
 EP0936787 (B1)[more >>](#)[Report a data error here](#)**Abstract of JP11316677**

**PROBLEM TO BE SOLVED:** To provide an authentication technique for the countermeasure of security used for a computer network by inserting a probe into at least one of plural files and identifying a position where the probing is executed in the computer network. **SOLUTION:** A communication traffic stream which enters and leaves a private network 130, etc., is consecutively monitored inside a fire wall 180. In this monitoring mode, a probe is inserted at random into a file arriving at the network 130. If this probing is executed at the client side, a signal is extracted to show a security warning. Thus, the wall 180 secures identification between the probe and a client and produces a security warning if a security warning showing the execution of a specific probe is received.

Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-316677

(43)公開日 平成11年(1999)11月16日

(51)Int.Cl.<sup>6</sup>  
 G 0 6 F 9/06  
 13/00  
 15/00  
 H 0 4 L 12/26

識別記号  
 5 5 0  
 3 5 1  
 3 3 0

F I  
 G 0 6 F 9/06  
 13/00  
 15/00  
 H 0 4 L 11/12

5 5 0 Z  
 3 5 1 Z  
 3 3 0 Z

審査請求 未請求 請求項の数28 O L (全 11 頁)

(21)出願番号 特願平11-15683

(22)出願日 平成11年(1999) 1月25日

(31)優先権主張番号 0 9 / 0 1 5 5 6 3

(32)優先日 1998年 1月29日

(33)優先権主張国 米国 (U S)

(71)出願人 596077259

ルーセント テクノロジーズ インコーポ  
レイテッドLucent Technologies  
Inc.アメリカ合衆国 07974 ニュージャージ  
ー、マレーヒル、マウンテン アベニュー  
600-700

(72)発明者 エリック グロッセ

アメリカ合衆国, 07922 ニュージャージ  
ー、パークレイ ハイツイ、ノース ロード  
140

(74)代理人 弁理士 三俣 弘文

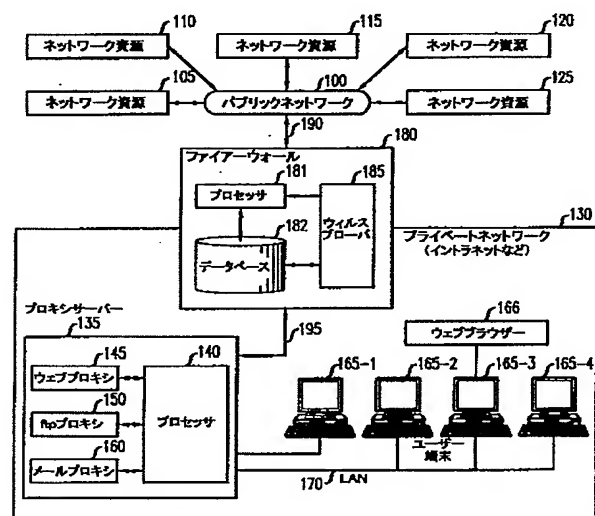
最終頁に続く

(54)【発明の名称】 コンピュータネットワークの保安方法

(57)【要約】

【課題】 ネットワークパフォーマンスを落とさないよ  
うなコンピュータネットワークにて用いられるセキュリ  
ティの対策の認証技術を提供する。

【解決手段】 コンピュータネットワーク内の特定のク  
ライアントがそのネットワークの所望のセキュリティ上  
の特徴に従って全体的に構成されているかどうかを判断  
する技術を提供する。ネットワーク内に入るファイル内  
にプローブがランダムに挿入される。プローブの挿入は  
コンピュータネットワークを他のネットワークから分離  
するファイアウォールにおいて行われる。プローブは  
特定の実行タスク（既知のウィルスなど）に従って構成  
し、適切に構成されたクライアントにおいてはプローブ  
は実行されず、ファイアウォールはセキュリティブリー  
チ（違反）を検出しない。不正な場合はプローブは実  
行されセキュリティアラートをトリガーさせる。



## 【特許請求の範囲】

【請求項1】 (A) コンピュータネットワークの通信トラフィックストリームを監視するステップと、前記通信トラフィックストリームは複数のファイルを含み、

(B) 前記複数のファイルのうち少なくとも1つのファイルへとプローブを挿入するステップと、

(C) 前記プローブがコンピュータネットワーク内で実行されたかを判断するステップと、

(D) プローブが実行された場合には、プローブの実行が行われたコンピュータネットワーク内の位置を識別するステップとを有することを特徴とするコンピュータネットワークの保安方法。

【請求項2】 コンピュータネットワーク内の識別された前記位置の情報を少なくとも含むセキュリティ警告を発生させるステップをさらに有することを特徴とする請求項1記載の方法。

【請求項3】 識別された前記位置は、コンピュータネットワーク内の複数のユーザー端末のうちの特定のユーザー端末であることを特徴とする請求項2記載の方法。

【請求項4】 前記プローブを挿入するステップ (B) は、コンピュータネットワーク内のサーバーが挿入することを特徴とする請求項1記載の方法。

【請求項5】 前記プローブは、トロイの木馬として構成するコンピュータウィルスであることを特徴とする請求項2記載の方法。

【請求項6】 前記通信トラフィックストリームは、通信ネットワークとパブリックネットワークの間を交換される際に前記サーバーを通過することを特徴とする請求項4記載の方法。

【請求項7】 前記プローブの実行は、特定のユーザー端末上を動作するウェブブラウザ上にて実行されることを特徴とする請求項3記載の方法。

【請求項8】 前記セキュリティ警告は、トロイの木馬が送信したUDPパケットがあったことに従って発生されることを特徴とする請求項5記載の方法。

【請求項9】 複数のユーザー端末を有するプライベートネットワークの保安方法であって、

(A) プライベートネットワークとパブリックネットワークとの間の通信トラフィックストリームを監視するステップと、  
前記通信トラフィックストリームは、複数のファイルを含み、前記複数のファイルの特定の1つのファイルは、前記複数のユーザー端末の特定の1つに対応付けられており、

(B) 複数のプローブの少なくとも1つのプローブを前記複数のファイルの特定の1つへと挿入するステップと、

(C) 前記ファイルが対応付けられたユーザー端末の特定の1つによりプローブが実行されたかどうかを判断す

るステップと、

(D) プローブが実行された場合には、プローブの実行が行われた前記ユーザー端末の特定の1つを識別するステップとを有することを特徴とする方法。

【請求項10】 前記少なくとも1つのプローブを挿入するステップは、プライベートネットワークとパブリックネットワークとの間に位置するファイアーウォールにおいて行われることを特徴とする請求項9記載の方法。

【請求項11】 (E) プローブからファイアーウォールへと識別された前記ユーザー端末の指示を少なくとも含んでいるセキュリティ警告を送信するステップをさらに有することを特徴とする請求項10記載の方法。

【請求項12】 前記プローブを挿入するステップ

(B) は、少なくとも1つのユーザー端末からパブリックネットワークへの最初のアクセスがあったことに従って行われることを特徴とする請求項10記載の方法。

【請求項13】 プローブは少なくとも1つのJava Script命令を含むことを特徴とする請求項12記載の方法。

【請求項14】 前記通信トラフィックストリームは、複数のTCP/IPパケットからなることを特徴とする請求項9記載の方法。

【請求項15】 プライベートネットワークとパブリックネットワークとの間のセキュリティを提供するファイアーウォールにおいて用いる方法であって、

(A) プライベートネットワークとパブリックネットワークとの間を送信される複数のパケットを含む通信トラフィックストリームを監視するステップと、

(B) 前記複数のパケットの少なくとも1つのパケットへとプローブを挿入するステップと、

(C) プライベートネットワークにおいてプローブが実行されたかどうかを判断するステップと、

(D) プローブが実行された場合に、プローブが実行されたプライベートネットワーク内の位置を識別するステップとを有することを特徴とする方法。

【請求項16】 プライベートネットワークは複数のユーザー端末を有するコンピュータネットワークであることを特徴とする請求項15記載の方法。

【請求項17】 前記位置を識別するステップ (D)

は、プローブが実行されたことを示す信号をプローブからファイアーウォールへと送信するステップからなることを特徴とする請求項16記載の方法。

【請求項18】 前記プローブを挿入するステップ

(B) は、少なくとも1つのユーザー端末からのパブリックネットワークへの最初のアクセスがあったことに従って行われることを特徴とする請求項16記載の方法。

【請求項19】 (A) プライベートネットワークとパブリックネットワークとの間を交換される複数のパケットへと複数のプローブを挿入するプローブと、

(B) 前記複数のパケットを監視し、かつ、前記複数の

プローブの特定のプローブがプライベートネットワークにおいて実行されたかを判断するプロセッサとを有することを特徴とするネットワークセキュリティ装置。

【請求項20】 (C) 前記複数のプローブを記憶するデータベースをさらに有することを特徴とする請求項19記載のネットワークセキュリティ装置。

【請求項21】 (D) 中央ソースから前記複数のプローブをダウンロードする通信チャネルをさらに有することを特徴とする請求項19記載のネットワークセキュリティ装置。

【請求項22】 (A) プライベートネットワークの入通信ストリームへと複数のプローブを挿入するステップと、

(B) プライベートネットワーク内の複数のユーザー端末に対して、前記複数のプローブの少なくとも1つのプローブが実行されたかを監視するステップとからなることを特徴とするネットワークの保安方法。

【請求項23】 (C) プライベートネットワーク内のプローブが実行された複数のユーザー端末のうちの特定のユーザー端末を識別するレポートを生成するステップをさらに有することを特徴とする請求項22記載の保安方法。

【請求項24】 前記複数のユーザー端末を監視するステップ(B)は、前記少なくとも1つのプローブの実行を示す信号をファイアーウォールへと送信するステップを有することを特徴とする請求項22記載の保安方法。

【請求項25】 前記複数のプローブを挿入するステップ(A)は、ファイアーウォール内にて行われることを特徴とする請求項24記載の保安方法。

【請求項26】 前記入通信ストリームはプライベートネットワークから入るストリームであることを特徴とする請求項24記載の保安方法。

【請求項27】 前記複数のプローブを挿入するステップ(A)は、プライベートネットワーク内の特定の資源にアクセスするプライベートネットワークからの要求があったことに従って行われることを特徴とする請求項26記載の保安方法。

【請求項28】 前記複数のプローブを挿入するステップは、少なくとも1つのユーザー端末からのパブリックネットワークへの最初のアクセスに従って行われることを特徴とする請求項26記載の保安方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークセキュリティに関し、特に、コンピュータネットワークにて用いられるセキュリティの対策(measure)の認証技術に関する。

【0002】

【従来の技術】通信技術における進歩およびパワフルなデスクトップコンピュータハードウェアを利用できるよ

10

20

30

40

50

うになったことにより、多くのパブリック的に(プライベートでないこと)利用可能なコンピュータネットワークにコンピュータをアクセスさせることが多くなってきた。今日では、インターネットのようなパブリックコンピュータネットワークを介して世界中のユーザー個人との間で莫大な量の情報が交換されている。ユーザーの分類の1つとして、会社内のインターネットのようなプライベートネットワークを介してお互い接続されたプライベートな個人および職業上のユーザーがある。プライベートコンピュータネットワークとパブリックコンピュータネットワークとの間での情報の交換によって、プライベートコンピュータネットワーク上の情報の保護およびプライベートコンピュータネットワーク自身の全体の機能に関して多くの非常に重要なセキュリティ問題を発生させた。

【0003】コンピュータネットワークセキュリティは、最低でも、コンピュータの運用およびネットワーク資源に対して信頼性を確実にし、不正な情報の流出や不正なアクセスからネットワーク内の情報を保護しなければならない。このようなネットワークセキュリティに対して多くのセキュリティ上の驚異を与える問題がますます増えている。そのセキュリティ上の驚異の内のもっとも洗練された種のもの、ネットワークコンピュータシステム内の特定の無防備なところを利用するプログラムがある。これらのプログラムに関連したセキュリティ上の驚異として周知な、論理爆弾(logic bomb)、トラップドア(trapdoor)、トロイの木馬(trojan horse)、ウィルス(virus)、ワーム(worm)などがある。これらは文献、W.Stallings, Network and Internetwork Security Principles and Practice, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1995.などに説明されている。

【0004】このような周知なソフトウェアプログラムの驚異は、セキュリティブリーチを達成するために独立に働くもの(例、ワーム)か、あるいは破壊的アクションを起こさせるためにホストプログラムを呼び出す必要があるもの(例、トラップドア、論理爆弾、トロイの木馬、ウィルス)がある。実際にこのようなプログラムは、十分に公知になるほどたくさんあり、プライベートネットワークコンピュータのセキュリティを不正にブリーチさせるのに用いられ、重大な損害を与えてしまっている。たとえば、文献、J.Hruska, Computer Viruses and Anti-Virus Warfare, Second edition, Ellis Horwood Limited, New York, 1992.に説明されている。このような損害としては、電子ファイルの破壊、データベースの変更、コンピュータネットワーク自身ないし影響を受けたコンピュータネットワーク自身ないし影響を受けたネットワークにつながれたコンピュータハードウェアを運用不能としてしまうことがある。

【0005】プライベートコンピュータネットワークの運用を行うネットワーク管理者は多くのセキュリティ対

策を用いて、コンピュータウィルスの侵入のような外的セキュリティブリーチからネットワークを保護しようとする。それらの技術の1つとしていわゆるファイアーウォールがある。このセキュリティ方式は、プライベートネットワークとパブリックネットワーク（インターネットなど）との間に別のコンピュータシステム（ファイアーウォール）を本質的に配置する。このファイアーウォールは、ソフトウェアベースのゲートウェイであり、外部のもの（認証されていないユーザー）による攻撃からLAN上のコンピュータを保護するように通常インストールされている。ファイアーウォールは、プライベートネットワークを出入りする通信を制御している。

【0006】ファイアーウォールは、プライベートネットワークを利用するすべてのユーザーに対して、特定のセキュリティ対策を与える。ファイアーウォールは新しいインターネットのサービスやワールドワイドウェブ（WWW）上の新しいサイトへのアクセスをブロックすることがある。なぜなら、その時点のファイアーウォールの構成にとってセキュリティ上及ぼされる結果が未知であったり登録されていなかったりするからである。ファイアーウォールの導入構成例として、WWWクライアントが直接WWWサーバに接触させない構成がある。この構成は通常制限が強すぎであり、従って、ネットワーク管理者はいわゆるプロキシサーバを利用することが多い。プロキシサーバは、ファイアーウォールを通してWWWクライアントからの要求を提供するような特定の機能があり、このようにして、インターネット上のサーバと出入りする通信の流れを提供する。

【0007】最近になり、ファイアーウォールのベンダーはいわゆるウィルスフィルタリング機能を提供するようになり、ウィルス感染に関連する重要なセキュリティ上の問題を解決している。このようにファイアーウォールにてウィルスフィルタリングを行うことは、クライアントマシン（PCなど）上で通常用いられている周知のウィルススキャンと概念的には同様なものであり、従来のクライアント／サーバ構成においてLAN内に存在させている。このようなクライアントベースのウィルス検出において、ウィルススキャンはクライアントのオペレーティングシステム、実行可能ファイル、システムファイル、ブートレコード、メモリなどを検索するプログラムを用いており、存在してはならないソフトウェアエンティティの存在を検出する。

【0008】コンピュータウィルスは、それらウィルスそれぞれがもっているウィルスシグネチャ（ウィルスの特徴）が前もって見つけられていてそれをウィルススキャナが用いることによって検出する。ウィルスシグネチャは、ウィルススキャンソフトウェアのベンダーが既知のウィルスから抽出した固定長シグネチャパターン（16～24バイトパターンなど）であることが多い。ウィルススキャンソフトウェアは既知のコンピュータウィル

スのシグネチャのリストをもっており、特定のクライアントのたくさんのファイルをスキャンし、特定のウィルスシグネチャと一致するかどうか検索する。もし一致していれば、クライアントのそのエンティティは感染したこととなり、それはユーザーに知らされる。

【0009】公知のファイアーウォール内でウィルスフィルタリングを行うことによりファイアーウォール内をファイルを伝送してスキャンングをしウィルス検出を行う。これはファイアーウォールにネットワークセキュリティ能力をさらに負荷するが、ファイアーウォールにおいてウィルスフィルタを実装することには運用上の問題がいくつかある。すなわち、（1）ファイアーウォールにて大量の処理を行わなければならない、待ち時間を発生させてしまいネットワークパフォーマンスを落としてしまい、ネットワークで実行しているアプリケーションに悪影響を与え、（2）ファイアーウォールはそれ自身はネットワークにおける個々のクライアントと比べて運用上およびデータインテリジェンスを少ない量しかもっておらず、クライアントベースのウィルススキャナで実行されるよりのファイアーウォールによっては到来するデータの正確なスキャンをすることができなくなる。

#### 【0010】

【発明が解決しようとする課題】従って、ファイアーウォールベースのウィルスフィルタリングの欠点を考えると、ファイアーウォール自身よりもネットワーク上のクライアントマシンにおいてウィルススクリーニングを行わせるネットワークセキュリティ管理者が多い。このようなクライアントベーススキャンングに対して現在はいくつかの有名な市販のコンピュータウィルススキャナが用いられている。ネットワークセキュリティ管理者は通常、特定の市販のウィルススキャンングプログラムを選択し、ネットワークのクライアントすべてにそのプログラムをインストールする。もちろんウィルススキャンングソフトウェアの有効性は導入の完全性および新しく発見されたウィルスに対応させたウィルスシグネチャリストにより周期的に更新することに大きく依存する。

【0011】非常に大きいクライアント／サーバネットワークにおいて、すべてのクライアント上でウィルス検出ソフトウェアが完全にインストールされていることを確実にする仕事は莫大であり達成できるかどうか分からない。クライアント同士の検査は多くの労働力を必要としてしまい、頻繁に行うことができない。従って、個々のユーザーがウィルススキャンングソフトウェアを更新する責任を通常持たされ、中央ソースからもっとも最近のウィルスシグネチャリストをダウンロードさせられる。この個々のユーザーが更新をしなかった場合にはもちろんネットワークはセキュリティブリーチの危険にさらされてしまう。

【0012】このように、コンピュータネットワーク全体を通してネットワークセキュリティ機能が完全に構成

10

20

30

40

50

されていることを確実にする必要がある。

#### 【0013】

【課題を解決するための手段】本発明は、コンピュータネットワーク内の特定のクライアントがそのコンピュータネットワークの所望のセキュリティ上の特徴に従って全体的に構成されているかどうかを判断する技術を提供する。本発明に従うと、コンピュータネットワーク内に入るファイル内にプローブがランダムに挿入される。プローブの挿入は、コンピュータネットワークを他のネットワークから分離するファイアーウォールにおいて行われる。

【0014】一態様に従うと、プローブは特定の実行タスク（既知のウィルスなど）に従って構成され、適切に構成されたクライアントにおいてはプローブは実行されず、ファイアーウォールはセキュリティブリーチ（違反）を検出しない。しかし、もしクライアントの構成が正しくない場合（すなわち、標準的ネットワークセキュリティ対策に従っていない場合）、プローブは実行され、ファイアーウォールにおいてセキュリティアラートをトリガーし（引き金を引き）、クライアントがセキュリティブリーチに無防備であることを指示する。ネットワークセキュリティ管理者は構成が正しくないクライアントを訂正するように適切な行動をとることができる。

【0015】好ましい実施例において、プローブはトロイの木馬の形態にてウィルスプローブとして構成される。このトロイの木馬は、実行すると、クライアントの構成が正しくないことを示す信号をファイアーウォールへと知らせる。別の実施例において、ファイアーウォールへ戻される信号は、ユーザーデータデータグラムプロトコル（UDP：User Datagram Protocol）パケットである。さらに別の実施例に従うと、特定のIPアドレスに対しブラウザーの種類からの最初のインターネットへのアクセスの際にウィルスプローブが挿入され、その後もウィルスプローブがランダムな時間間隔で挿入される。

#### 【0016】

【発明の実施の形態】図1は、本発明の原理を用いるシステムを示している。このシステムは、パブリックネットワーク100（インターネットなど）、ネットワーク資源105、ネットワーク資源110、ネットワーク資源115、ネットワーク資源120、ネットワーク資源125を有する。ネットワーク資源105～ネットワーク資源125は、周知のHTML言語により書かれたファイルによってリンクすることができ、周知のWWWを表す。WWWとHTMLは文献、B. White, HTML and the Art of Authoring for the World Wide Web, Kluwer Academic Publishers, Norwell, MA, 1996. などに説明されている。

【0017】プライベートネットワーク130は特定のユーザーサイト（会社の本社ビルなど）内に位置するネ

ットワークであり、LAN170によってユーザー端末165-1、165-2、165-3、165-4がつながれている。ユーザー端末165-1～165-4はスタンドアローンのパーソナルコンピュータやネットワーク端末であってもよい。

【0018】簡明さのため、図1においては1つのLAN構成しか示していないが、プライベートネットワーク130はLAN170と同様な複数のLAN構成を含んでいてもよい。ユーザー端末165-1～165-4のいずれの特定のユーザーもWWW（ネットワーク資源105～ネットワーク資源125など）上で利用可能な特定の資源を要求するためにユーザー端末165-2などでクライアントプログラムを実行させる。前述のように、プライベートネットワーク130からインターネットを介してのWWWへのこのような要求はプライベートネットワーク130とユーザー端末165-1～165-4との両方にセキュリティ上の危険を与える。

【0019】図1に示すように、プライベートネットワーク130はファイアーウォール180およびプロキシサーバー135を有し、これらは本発明に従って特定のセキュリティ機能を提供するように構成され、プライベートネットワーク130およびその多くのコンピュータ資源を保護する。

【0020】前述のように、プライベートコンピュータネットワーク（130など）の運用に責任があるネットワーク管理者はたくさんのセキュリティ対策を用いて、コンピュータウィルスの侵入のような外的セキュリティブリーチからネットワークを保護する。その技術の1つとして、プライベートネットワークとパブリックネットワーク（インターネットなど）との間に別のコンピュータシステム（ファイアーウォール）を開示するものがある。ファイアーウォールを用いるプライベートネットワークにおいて、ファイアーウォールはまず、プライベートネットワークのユーザー端末とパブリックネットワークとの間の要求された接続が認証されるものかどうかを判断する。

【0021】ファイアーウォールはプライベートネットワークにおけるユーザー端末とパブリックネットワークとの間の中間体として機能し、もしその接続が認証されると、それら2つのネットワークの間の接続を可能にする。逆に、接続が認証されなければ、ファイアーウォールはそれらネットワークの間の接続を実現させない。

【0022】図1の実施例に従うと、プロキシサーバー135はプロセッサ140、ウェブプロキシ145、ftpプロキシ150、メールプロキシ160を有する。これらのプロキシはファイアーウォールと共に働くプロキシサーバーがそれぞれ、WWW/インターネットアクセス、ファイル転送、電子メールに対してセキュリティ機能を提供する。例として、ウェブプロキシ145はユーザーがWWW上の特定のウェブページにプライベ

10

20

30

40

50

ートネットワーク130からアクセスしたいと望む場合に用いられる。ユーザー端末165-2を用いるユーザーはウェブブラウザ166を用いてWWW上の特定のウェブページにアクセスすることができる。ウェブブラウザは周知のソフトウェアアプリケーションプログラム(Netscape Communications社のNetscape Navigator(登録商標v.5.0)など)であり、WWW上をネットサーフィンすることを可能にし、WWW上の最良の情報にアクセスすることを可能とする。

【0023】ウェブブラウザ166はユーザー端末165-2のユーザーから入力要求を受信し、WWW上の適切な資源(ネットワーク資源105など)とパブリックネットワーク100を通して接続を確立することによりWWW上の情報を位置決めしようと試みる。ユーザー端末165-2とネットワーク資源105との間の接続はプロキシサーバー135、ウェブプロキシ145、ファイアウォール180を用いて確率される。ウェブブラウザ166のために働くウェブプロキシ145は、ユーザー端末165-2とネットワーク資源105の間のTCP/IP接続を確立しようと試みる。

【0024】TCP/IPは、インターネットを情報伝送する方法に用いられるプロトコルであり周知である。TCP/IPは、情報を個別のパケットの分離し、送り側のコンピュータ(サーバーなど)と受け側のコンピュータ(クライアントなど)との間をこれらのパケットをルーティングする。TCP/IPおよびインターネット通信は文献、D. Comer, Internetworking with TCP/IP Third edition, Prentice-Hall, Englewood Cliffs, NJ, 1995.などに説明されている。好ましい実施例において、ユーザー端末165-2とネットワーク資源105との間のTCP/IP接続は、それぞれ、通信チャンネル190、195をまたがって設けられる。これらはパブリックネットワーク100、プライベートネットワーク130、さらに、ユーザー端末165-2との間の接続を確立する。

【0025】図1に示すように、パブリックネットワーク100とプライベートネットワーク130の間の通信トラフィックすべては、ファイアウォール180を通る必要がある。この通信トラフィックの寄与を考えると、発明者は、本発明のセキュリティ上の利点を実装するために、ファイアウォール180が好ましい位置であることを認識した。好ましい実施例に従うと、ファイアウォール180はプロセッサ181、データベース182、パブリックネットワーク100などからプライベートネットワーク130などへと到来するファイル内にプローブをランダムに挿入するウィルスプローバ185を含んでいる。ウィルスプローバ185が挿入するプローブは実行すると特定の動作をトリガーする個別のプログラムである。

【0026】一実施例に従うと、プローブはトロイの木

馬として構成するウィルスプローブである。これは、クライアントの構成が正しくないことを示す信号をファイアウォールへと送り返す。コンピュータウィルスの観点からは、トロイの木馬は、コンピュータハッカー、コンピュータクラッカーのような不正ユーザーがアプリケーションプログラムに配置した秘密でドキュメント化されていないエントリーポイントである。ユーザーがそのアプリケーションプログラムを実行すると通常、トロイの木馬もまた実行され、望ましくない動作を起こさせる。

【0027】トロイの木馬は文献、Stallings, supra, pp. 238-241.などに説明されている。例として、トロイの木馬は共有コンピュータシステム上の別のユーザーのファイルへのアクセスを容易になるように作られ、不正ユーザーが正当なユーザーのファイル権限を実行した場合に変えてしまい、どのユーザーにも読み取り可能なファイルとしてしまう。この実施例において、後述するように、トロイの木馬の特定の機能を用いてコンピュータネットワークにとって利点となるセキュリティの徹底を行う。

【0028】ファイアウォール180にてウィルスプローバ185により挿入されたウィルスプローブは、そのプローブが実行されるとファイアウォール180へと信号を送り返すように設計され、従来考えられているトロイの木馬の感覚で起こるような破壊的な動作ではない動作を実行する。本発明のセキュリティ機能はファイアウォール(180など)にて実装され実現される。なぜなら、ファイアウォールが用いられているネットワークにおいてすべての通信トラフィックはファイアウォールを通過しなければならないからである。従ってファイアウォールは本発明に従ってプローブを挿入する理想的な位置である。

【0029】しかし本発明の原理は他のネットワーク環境や構成にても実現することができる。例えば、一般アクセスが高い割合であり信頼性が高いことで知られているネットワーク内の特定のプロキシサーバーを用いてプローブの挿入を実現することができる。例として、オンライン電話帳を主として提供するプライベートネットワーク内の信頼性が高いサーバーもまた本発明の原理を実装するのに適している。なぜなら、このサーバーはプライベートネットワーク内の多くのユーザーにより用いられるからである。従って、本発明により分配されるセキュリティ機能は図1のシステム構成のようなシステムであるか否かに関わらず多くのネットワーク、ハードウェア、ソフトウェア構成にて実現することができる。

【0030】本発明に従ってプローブを挿入、監視、実行することによりネットワークセキュリティを提供する動作を図2に示した。好ましい実施例に従うと、上述のように、図2の動作はファイアウォール180内で開始する。プライベートネットワーク130などを出入り



する通信トラフィックストリームが継続的に監視される(200)。ネットワーク上を伝送される通信トラフィックストリームを監視の際に、プライベートネットワーク130に向かって到来するファイルへとプローブがランダムに挿入される(205)。本発明のプローブの構造的観点、図3とともに後で説明する。本発明に従うと、クライアント上で実行された場合、セキュリティ警告を示す信号を取り出すようにプローブは設計される。

【0031】信号はネットワーク資源の要求であることがある。このような要求はすべてファイアーウォールを通過して行われるので、本発明に従って構成するプローブがこのような要求をトリガーするとその要求がファイアーウォールへの信号として有効に用いられることを確実にする。すなわち、プローブがトリガーするこのような信号はファイアーウォールにより直ちに認識することができる。別の実施例において、信号は従来技術のユーザーデータグラムプロトコル(UDP)パケットの形態とすることができる。UDPは従来のTCP/IPプロトコル上の最上層のコンネクションレス型の転送プロトコルであり、少ない量のデータを迅速に2つのアプリケーションが交換するのに低いオーバーヘッドメカニズムを提供している。

【0032】UDPは通常のTCP/IPパケット交換よりも少ないオーバーヘッドしか必要としない。なぜならUDPはTCP/IPよりもセキュリティが弱いプロトコルであるからである。すなわち、UDPは伝送指向であり、パケットは複製されたり、迷子になったり、別の順番で受信されたりしてしまう。逆にTCP/IPはより信頼性が高い。なぜなら宛先に正確に完全に到来することを確実にするためにある程度の大きさの長さをもっているからである(チェックサムを生成したり、パケットの受け取り確認をしたり、迷子パケットを再送信したりすることなど)。UDPはこのようなオーバーヘッドはもっていないのでTCP/IPよりもある程度速く、本発明の多くの実施例におけるのと同様に、短いデータバーストを送ったり、速いネットワークスループットを必要としたり、宛先に配信の確認を必要としないようなアプリケーションにとっては理想的である。これら上述の信号構成の他の信号構成であっても本発明の原理を有効に提供することができる。

【0033】このように、ファイアーウォール180は特定のプローブが実行されたというセキュリティ警告指示(UDPパケットなど)を受信し、ファイアーウォールはプローブとクライアントを同定し(215)、セキュリティ警告を発生させる(220)。生成されたセキュリティ警告の特性および種類は、本発明に従うと、いろんな形態であってもよい。ファイアーウォール180が生成したセキュリティ警告は、ネットワーク内の特定のクライアントに現在セキュリティ危機が存在することを示すネットワーク管理者への直ちに送られるメッセー

ジとすることができる。一実施例において、ネットワーク内のいろんなクライアントによりプローブが実行されると、マスターファイルにログエントリを作成しデータベース182などに記憶される。これは周期的にネットワーク管理者によりアクセスすることができ、あるいはそのログを管理者が見ることができるようにレポートを印刷するようにしてもよい。

【0034】本発明は、コンピュータネットワーク内の特定のクライアントがそのコンピュータネットワークの望ましいネットワークセキュリティ機能に従って完全に構成しているかどうかを判断する技術を提供することができる。例えば、ほとんどのネットワーク管理者により行われている従来のセキュリティ対策はネットワーク

(130など)内のすべてのユーザーにウェブブラウザソフトウェア(Netscape Navigator(登録商標)など)の特定の機能を使えなくするポリシーであり、特に、ウェブブラウザのJavaScriptインタープリター機能を使えなくする。JavaScript(商標)は例えば文献、D.Flanagan, Javascript The Definitive Guide, Second edition, O'Reilly & Associates, Sebastopol, CS, 1997.に説明されている。JavaScriptは、ユーザーやHTMLを伴うプログラムを開発したりするのによく用いられる周知のインタープリター型プログラミング言語である。例えば、ウェブブラウザがJavaScriptインタープリターを具備すれば、そのウェブブラウザはJavaScriptの「スクリプト」の形態でインターネット(およびWWW)上を実行可能なコンテンツ(プログラムなど)を配信することを可能にする。

【0035】スクリプトがJavaScriptを実行できるブラウザにロードされると、スクリプトは実行可能となり、そのスクリプトのJavaScript命令に規定されるような特定の出力を作る。従って、JavaScriptはウェブブラウザの制御を支配することができ、また、ウェブページに現れるコンテンツ(HTMLフォームなど)の制御をも支配する。公知のように、JavaScriptを用いて可能となるこれらの機能は重大なネットワークセキュリティ上の危険を発生させる。

【0036】上述のようなウェブブラウザ環境に本発明を導入することを以下の実施例により説明する。図1および3において、プライベートネットワーク130はユーザー端末165-1~165-4を用いる複数のユーザーを含んでいる。前述のように、ユーザー端末それぞれはユーザー端末165-2上を実行するウェブブラウザ(160など)を具備するように構成することができる。ユーザー端末165-2の構成は他のプライベートネットワーク内の他のユーザー端末それぞれの上において容易に複製することができるが、簡明さのため図1においては一部のみを示した。

【0037】プライベートネットワーク130のセキュリティポリシーに適合するように、外部のソース（パブリックネットワークなど）から導入され、プライベートネットワークを多くのセキュリティ上の危険にさらすようなスクリプトの実行を防ぐためにすべてのウェブブラウザはJavaScriptインタプリタを使えないようにされる。もちろんこのようなセキュリティ対策はネットワークユーザーが従った場合にのみ有効である。多くのプライベートネットワークにおいて、このようなセキュリティ対策に従わないようなユーザー端末が存在してしまう。これらの従わないユーザー端末はネットワーク全体をセキュリティ上の危険にさらし、ネットワーク管理者にとってはプライベートネットワーク全体ですべてのセキュリティ対策に完全に適合させるため常に格闘しなければならなくなっている。

【0038】前述のように、本発明はコンピュータネットワーク内のクライアントがそのコンピュータネットワークの望ましいネットワークセキュリティ機能に完全に従っているかどうかを判断する技術を提供する。ファイアーウォール180が本発明に従って構成され、プライベートネットワーク130への入通信トラフィックストリームへとプローブを挿入する。図3は、入通信トラフィックストリーム300の例を示し、本発明に従ってプローブを挿入している例を示している。通信トラフィックストリーム300はパブリックネットワーク100からプライベートネットワーク130へとデータを運ぶ一連の個々のパケット300-1からパケット300-N（TCP/IPパケットなど）を含んでいる。本発明に従うと、ファイアーウォール180はパケット300を監視し、パケットの間に入ファイルへとプローブをランダムに挿入する。例としてパケット300-4は入ファイル305を含み、これは一連のHTML命令310を含むファイルである。

【0039】ウィルスプローバ185がプローブ315をHTML命令310の終わりに挿入する。いくつかの実施例に従うと、特定のIPアドレス（クライアント）ないしブラウザ種類からの最初のインターネットへのアクセスの際にプローブ315が挿入され、その後はランダムな感覚でウィルスプローブが挿入される。プローブ315はトロイの木馬の形態のウィルスプローブであり、ファイル305へとプローブ315を挿入すると編集済みファイル325となる。その後、プライベートネットワーク130への通信トラフィック300の伝送において編集済みファイル325により進行する。

【0040】プローブ315は単一のJavaScript命令320である。320は、<SCRIPT>x=new image();x.src='image1';</SCRIPT>の形態であり、これはウェブブラウザを制御するインタプリタ型スクリプト言語の文である。image1はプローブ315を識別する固有な文字列である。プローブ315は基本的に

はトロイの木馬であり、ウェブブラウザに対し、オフスクリーンビットマップスペース（new image()）を配置し、小さなイメージ（image1）をダウンロードさせるように命令する。プローブは、ウィルスプローバ185によるアクセスのためデータベース182に記憶してもよいが、ウィルスプローバ185自身にローカルに記憶してもよい。別の実施例では、中央ソース（インターネットなど）からプローブをネットワーク管理者によりダウンロードさせ、現存するプローブライブラリーに加えてもよい。

【0041】もしウェブブラウザ166が、すべてのウェブブラウザにJavaScriptインタプリタを使えなくさせるというネットワークセキュリティ機能に適合していれば、プローブ315は実行されず、ファイアーウォール180はセキュリティ警告を生成しない。しかし、もしウェブブラウザ166の構成が誤っていれば、プローブ315は実行され、ウェブブラウザ166にイメージファイル（image1）の要求を開始させる。このようなまれなウェブブラウザ166によるネットワーク資源の要求はファイアーウォール180により捕獲され、セキュリティ警告の信号として機能する。適切に構成されたウェブブラウザではこのようにネットワーク資源（image1）を要求することは、適切に構成されていなかったり確立されたネットワークセキュリティ対策に違反している場合をのぞいてはない。すなわち、プローブ315の実行はプライベートネットワーク130の望ましいセキュリティ対策に適合していないようにウェブブラウザ166がJavaScriptを使えるようになっていたことを意味し、これはネットワークにセキュリティ上の危機を与えることを意味する。

【0042】別の実施例において、本発明は、セキュリティ警告が起こったときにファイアーウォールへ戻す信号としてUDPパケットを用いる。ファイル305は特定の実行可能命令を含むファイルである。拡張子が、.exeであるファイルはバイナリー実行可能ファイルである。プローブ315はファイル305の少量のバイトをプローブ315を挿入することによって書き換えてしまうのに安全である適切な位置にファイル305へと挿入される。

【0043】この実施例では、プローブ315はセキュリティ警告が発生した場合にUDPパケットを発する。ファイル305へと挿入される実際の機械設命令は周知のプログラミング言語Cで書かれた以下のコード部分を用いる（コンパイルする）ことにより生成することができる。

```
struct sockaddr_in sin={0,9,{0xF14E8A11},0,0,0,0,0,0,0,0};
ints=socket(PF_INET,SOCK_DGRAM,0);
connect(s,&sin,sizeof(sin));
```

```
write(s, 0x88, 1);
close(s);
```

【0044】上のC言語のコード部分を機械語コードへとコンパイルすると、これはプローブ315としてファイル305へと挿入され、プローブを実行した際に所望のUDPパケットを生成する。すなわち、もしプローブ315を特定のユーザー端末上で実行すると、そのユーザー端末がセキュリティ上の危険をはらんでいることを示す信号として、ファイアーウォール180へとUDPパケットが発せられる。

#### 【図面の簡単な説明】

【図1】本発明の原理を用いるシステムのブロック図である。

【図2】本発明を用いる図1のファイアーウォールが実行する動作の流れ図である。

【図3】図1のシステムで送信される通信トラフィックストリームである。

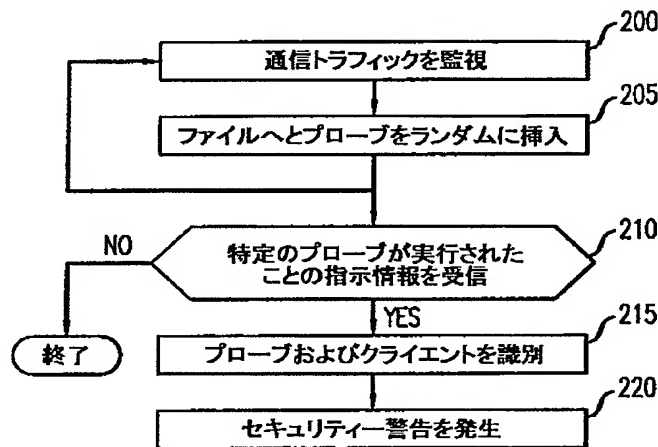
#### 【符号の説明】

100 パブリックネットワーク  
105 ネットワーク資源  
110、115 ネットワーク資源  
120、125 ネットワーク資源  
130 プライベートネットワーク  
135 プロキシサーバー

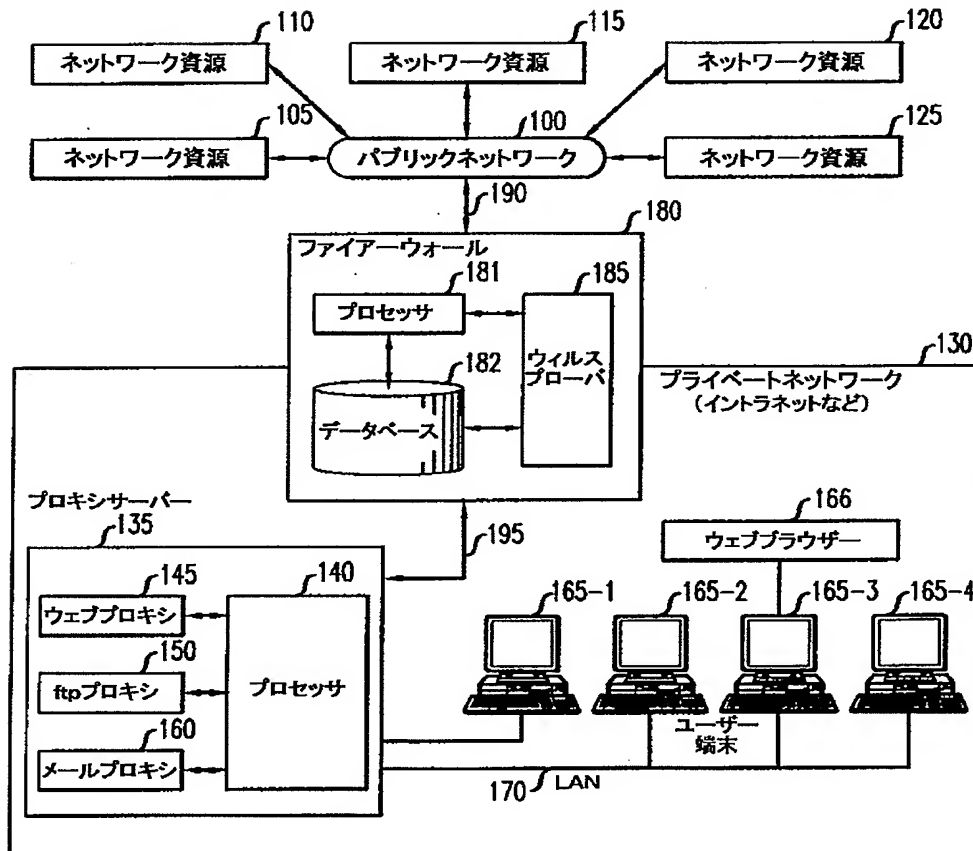
\* 140 プロセッサ  
145 ウェブプロキシ  
150 ftpプロキシ  
160 メールプロキシ  
165 ユーザー端末  
166 ウェブブラウザ  
170 LAN  
180 ファイアーウォール  
181 プロセッサ  
182 データベース  
185 ウィルスプローバ  
200 通信トラフィックを監視  
205 ファイルへとプローブをランダムに挿入  
210 特定のプローブが実行されたことの指示情報を受信  
215 プローブおよびクライアントを識別  
220 セキュリティー警告を発生  
300 パケット  
305 HTMLファイル  
310 HTML命令  
315 プローブ  
320 JavaScript命令  
325 編集済みファイル

\*

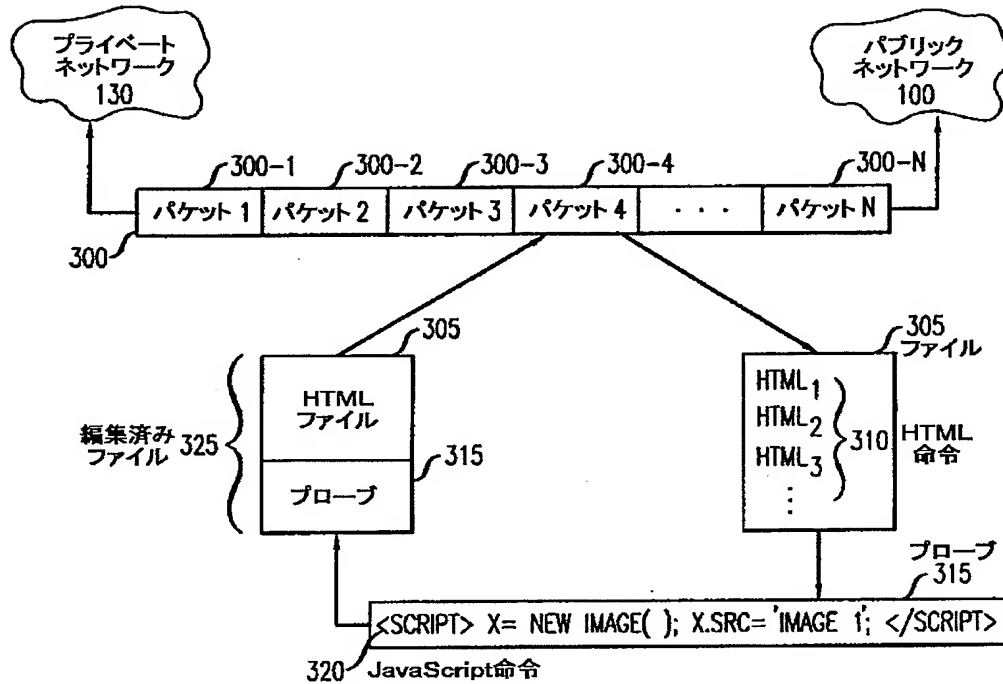
【図2】



【図1】



【図3】



フロントページの続き

(71)出願人 596077259  
 600 Mountain Avenue,  
 Murray Hill, New Je  
 rsey 07974-0636U. S. A.